| [Document Name] | Patent Application Request |
|---|---|
| [Reference Number] | 84026 |
| [Filing Date] | February 5, 2004 |
| [Destination] | Commissioner of Patent Office |
| [International Patent Classification] | G06F 9/00 |
| | H04B 17/00 |

[Inventor]

    [Domicile or Residence]    c/o Trend Micro Incorporated, 2-1-1, Yoyogi, Shibuya-ku, Tokyo

    [Name]    Satoshi KONDO

[Inventor]

    [Domicile or Residence]    c/o Trend Micro Incorporated, 2-1-1, Yoyogi, Shibuya-ku, Tokyo

    [Name]    Shigeru YATABE

[Applicant]

    [Identification Number]    397011166

    [Name]    Trend Micro Incorporated

[Agent]

    [Identification Number]    100098084

    [Patent Attorney]

    [Name]    Kenji KAWASAKI

[Selected Agent]

    [Identification Number]    100111763

    [Patent Attorney]

    [Name]    Takashi MATSUMOTO

[Fee Detail]

    [Deposit Number]    038265

    [Amount]    21,000 yen

[Attachment(s)]

| [Item] | Claim | 1 |
|---|---|---|
| [Item] | Description | 1 |
| [Item] | Drawing | 1 |
| [Item] | Abstract | 1 |

[Document Name] Claim
[Claim 1]
   A receiving device comprising:

   registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used;

   receiving means for receiving a program and function information indicating a function used in the program;

   determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether a program received by the receiving means includes a function not permitted to be used; and

   outputting means for outputting a result determined by the determining means.
[Claim 2]
   A receiving device comprising:

   registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used;

   receiving means for receiving a program and function information indicating a function used in the program;

   determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether to execute a program received by the receiving means; and

   executing means for executing the program if the determining means determines to execute the program.
[Claim 3]
   A receiving device comprising:

   registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used;

   receiving means for receiving a program and function information indicating a function used in the program;

   determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether to execute a program received by the receiving means; and

   outputting means for outputting a message asking whether to execute a program while limiting available functions, if the determining means does not allow execution of the program.

   operating means;

   executing means for executing the program if execution of the program is instructed via the operating means in response to a message outputted by the outputting means; and

   limiting means for limiting functions available in a program executed by the executing means, in accordance with information registered by the registering means.
[Claim 4]
   A receiving device according to Claim 2 or 3, wherein

   the determining means compares the function information received by the receiving means and the information registered by the registering means, and if a function not permitted to be used is

not used by the program received by the receiving means, permits execution of the program.
[Claim 5]

A receiving device according to any one of Claims 1 to 3, wherein:

the registering means registers information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used; and

the function information is information on a function contained in the program received by the receiving means.
[Claim 6]

A receiving device according to any one of Claims 1 to 3, wherein:

the registering means registers information indicating a resource permitted to be accessed in accordance with a received program or information indicating a resource prohibited from being accessed in accordance with the program; and

the function information is information indicating a resource accessed in accordance with the program received by the receiving means.
[Claim 7]

A receiving device comprising:

registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used;

first receiving means for receiving, before receiving a program, function information indicating a function used in the program;

determining means for determining whether to receive a program, by comparing function information received by the first receiving means and information registered by the registering means;

second receiving means for receiving a program if the determining means allows receipt of the program; and

executing means for executing a program received by the second receiving means.
[Claim 8]

A relay device comprising:

registering means for registering information indicating a function of a program provided via a network, permitted to be used or information indicating a function of the program prohibited from being used;

receiving means for receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program;

determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether to relay a program received by the receiving means; and

sending means for sending the program to a destination designated by destination information received by the receiving means, if the determining means allows relay of the program.
[Claim 9]

A relay device according to Claim 8, wherein

the determining means compares the function information received by the receiving means and the information registered by the registering means, and if a function not permitted to be used is not used in the program received by the receiving means, permits relay of the program.

[Claim 10]

A relay device comprising:

registering means for registering information indicating a function of a program provided via a network, permitted to be used or information indicating a function of the program prohibited from being used;

receiving means for receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program;

determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether a function not permitted to be used is used in a program received by the receiving means; and

sending means for sending a determination result by the determining means and the program to a destination designated by destination information received by the receiving means.

[Claim 11]

A relay device according to Claim 8 or 10, wherein:

the registering means registers information indicating a function of a program provided via a network, permitted to be used or information indicating a function of the program prohibited from being used; and

the function information is information on a function contained in the program received by the receiving means.

[Claim 12]

A relay device according to Claim 8 or 10, wherein:

the registering means registers information indicating a function of a program provided via a network, permitted to be accessed or information indicating a function of the program prohibited from being accessed; and

the function information is information on a resource accessed in accordance with the program received by the receiving means.

[Claim 13]

A program for causing a computer to execute:

a first step of receiving a program and function information indicating a function used in the program;

a second step of determining, by comparing function information received in the first step and information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used, which is pre-registered in memory, whether a function not permitted to be used is used in a program received in the first step; and

a third step of outputting a determination result in the second step.

[Claim 14]

A program for causing a computer to execute:

a first step of receiving a program and function information indicating a function used in the program;

a second step of determining, by comparing function information received in the first step and information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used, which is pre-registered in memory, whether to execute a program received in the first step; and

a third step of executing a program if the execution of the program is permitted in the second step.

3

[Claim 15]

A program for causing a computer to execute:

a first step of receiving, before receiving a program, function information indicating a function used in the program;

a second step of determining, by comparing function information received in the first step and information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used, which is pre-registered in memory, whether to receive a program associated with the function information;

a third step of receiving a program if receipt of the program is allowed in the second step; and

a fourth step of executing a program received in the third step.

[Claim 16]

A program for causing a computer to execute:

a first step of receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program;

a second step of determining, by comparing function information received in the first step and information indicating a function of a program provided via a network, permitted to be used or information indicating a function of the program prohibited from being used, which is pre-registered in memory, whether to relay a program received in the first step; and

a third step of sending the program to a destination designated by destination information received in the first step, if relay of the program is allowed in the second step.

[Claim 17]

A program for causing a computer to execute:

a first step of receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program;

a second step of determining, by comparing function information received in the first step and information indicating a function of a program provided via a network, permitted to be used or information indicating a function of the program prohibited from being used, which is pre-registered in memory, whether a function not permitted to be used is used in a program received in the first step; and

a third step of sending a determination result in the second step and the program to a destination designated by destination information received in the first step.

[Claim 18]

A computer-readable storage medium recording a program according to any one of Claims 13 to 17.

[Document Name] Description
[Title of Invention] Security Ensuring by Program Analysis on Information Device and Transmission Path
[Technical Field]

[0001]

The present invention relates to a technique for ensuring security of an information device.

[Background Art]

[0002]

In an open network such as the Internet, people can freely publicize information or provide programs. Accordingly, there exists a possibility of a malicious program being provided via an open network to a communication terminal, and which if executed will result in a security breach with information stored in the terminal being read and sent out from the terminal. In order to protect communication terminals from such programs, for example, a program executing device described in patent document 1 registers identification information (for example, an IP address or a URL) indicating reliable sources of programs, in a memory, and if identification information indicating a source of a program received via a network is registered in the memory, permits execution of the program.

[Patent Document 1] JP2001-117769A

[Disclosure of Invention]
[Problem to be Solved by Invention]

[0003]

However, in the art disclosed in patent document 1, it is necessary to register all reliable program sending sources. Accordingly, each time a reliable program sending source is added or deleted, identification information stored in a memory must be updated. Moreover, since in a large network such as the Internet, there exists a large number of reliable program sending sources, it is substantially difficult to register in a memory of a terminal all identification information thereof. Further, even if it is possible to register in a memory in a terminal all such identification information, in order to do so it is necessary to increase a size of a memory used, particularly of that in a small communication terminal such as mobile phone, which results in an increase in manufacturing costs of such a terminal.

[0004]

On the other hand, in order to analyze at a mobile terminal a content of a program received at the mobile terminal via a network to determine whether the program is a security threat, it is necessary for the mobile terminal to have a high level of computing power. Moreover, determination of security threats at the mobile terminal places a heavy load on a processing unit of the mobile terminal and takes a substantial amount of time to complete. Similarly, if at a relay device such as a server on a network, a content of a program received via a network is analyzed to thereby determine whether execution of the program in a communication terminal will constitute a security threat, it is necessary to provide the relay device with a high level of computing power. If the relay device is not provided with sufficient computing power, delays in communications are likely to occur.

[0005]

The present invention has been made in view of the problems discussed above, and provides a technique of determining, at a receiving device or a relay device, whether a program provided via a network is a security threat, by using a simple method which can be quickly carried out.

[Means for Solving Problem]

[0006]

To solve the problems, the present invention provides a receiving device comprising: registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used; receiving means for receiving a program and function information indicating a function used in the program; determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether a program received by the receiving means includes a function not permitted to be used; and outputting means for outputting a result determined by the determining means.

[0007]

The present invention also provides a program for causing a computer to function as a receiving device, and provides a computer-readable storage medium for recording the program. The program may be pre-installed in a memory of a computer, or it may be installed in a computer by way of communications conducted via a network, or be installed from the storage medium.

[0008]

According to the present invention, a receiving device determines whether a prohibited function is present in a received program by comparing function information of the program and information registered by the registering means, and outputs the determination result.

[0009]

The present invention also provides a receiving device comprising: registering means for registering information indicating a function of a received program permitted to be used or information indicating a function of the program prohibited from being used; receiving means for receiving a program and function information indicating a function used in the program; determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether to execute a program received by the receiving means; and executing means for executing a program if the determining allows execution of the program.  The present invention also provides a program for causing a computer to function as a receiving device, and provides a computer-readable storage medium for recording the program.

[0010]

According to the present invention, a receiving device determines whether a received program should be executed by comparing function information of the program and information registered by the registering means.

[0011]

The present invention also provides a receiving device comprising: registering means for registering means for registering information indicating a function of a received program is permitted to be used or information indicating a function of the program prohibited from being

2

used; first receiving means for receiving, before receiving a program, function information indicating a function used in the program; determining means for determining whether to receive a program, by comparing function information received by the first receiving means and information registered by the registering means; second receiving means for receiving a program if the determining means allows receipt of the program; and executing means for executing a program received by the second receiving means. The present invention also provides a program for causing a computer to function as a receiving device, and a computer-readable storage medium for recording the program.

[0012]

According to the present invention, a receiving device determines whether a program should be received by comparing function information of the program and information registered by the registering means.

[0013]

The present invention provides a relay device comprising: registering means for registering information on indicating a function of a program provided via a network permitted to be used or information indicating a function of the program prohibited from being used; receiving means for receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program; determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether to relay a program received by the receiving means; and sending means for sending a program to a destination designated by destination information received by the receiving means, if the determining means allows relay of the program.

[0014]

The present invention also provides a program for causing a computer to function as a relay device, and provides a computer-readable storage medium for recording the program. The program may be pre-installed in a memory of a computer, or it may be installed in a computer by way of communications conducted via a network, or be installed from the storage medium.

[0015]

According to the present invention, a relay device determines whether to relay a received program by comparing function information of the program and information registered by the registering means.

[0016]

The present invention also provides a relay device comprising: registering means for registering information indicating a function of a program provided via a network permitted to be used or information indicating a function of the program prohibited from being used; receiving means for receiving a program, function information indicating a function used in the program, and destination information indicating a destination of the program; determining means for determining, by comparing function information received by the receiving means and information registered by the registering means, whether a function not permitted to be used is used in a program received by the receiving means; and sending means for sending a determination result by the determining means and a program to a destination designated by destination information received by the receiving means. The present invention also provides a program for causing a computer to

3

function as a relay device, and provides a computer-readable storage medium for recording the program.

[0017]

According to the present invention, a relay device determines whether a prohibited function is present in a received program by comparing function information of the program and information registered by a registering means, and sends the determination result with the program.

[0018]

According to the present invention, it can be readily determined at a receiving device or a relay device whether a program provided via a network is one that poses a security threat, by employing a simple method and within a short time.

[Best Mode for Implementing Invention]

[0019]

Below, with reference to the drawings, embodiments of the present invention will be described.

[A. First Embodiment]

Fig. 1 is a block diagram illustrating a configuration of communication system according to the first embodiment.   In Fig. 1, content provider 10 is a service provider that provides content to mobile phone 50.   Content server 10a conducts packet communication with mobile phone 50 via Internet 30 and mobile packet communication network 40.   Content server 10a stores programs for mobile phone 50 and inspection result data 202 which are obtained as a result of inspection of the program in inspection institution 20.   The programs stored in content server 10a may be software containing image or audio data used when a program is executed.

[0020]

Inspection institution 20 is an institution which inspects a program provided to mobile phone 50 upon an inspection request from content provider 10, and program inspection device 20a stores security evaluation list 201.   In security evaluation list 201 there are listed functions such as a function call and a system call which may compromise security in mobile phone 50 if provided with a program via a network and the program is executed.   Security evaluation list 201 also lists resources accessible by mobile phone 50 which may compromise security in mobile phone 50 if accessed in accordance with a program provided via a network.

[0021]

Program inspection device 20a analyzes a program to be inspected with reference to security evaluation list 201, and extracts from the program functions listed in security evaluation list 201.   Program inspection device 20a also identifies, among resources accessed when the program is executed, resources listed in security evaluation list 201.   Subsequently, program inspection device 20a generates inspection result data 202 containing the names of the extracted functions and information on the identified resources (for example, URLs or paths indicating where the resources have been stored or identifiers assigned to the resources).   Inspection result data 202 is returned to content provider 10 and stored along with the program in content server 10a.

[0022]

Program inspection device 20a may record as inspection result data 202 all functions contained in a program to be inspected, or may record all resources accessed when a program to be

inspected is executed.

[0023]

Mobile phone 50 is a communication terminal (receiving device) served by mobile packet communication network 40, and can download a program from content server 10a and execute it.

[0024]

Fig. 2 is a diagram illustrating a data structure of inspection result data 202. As shown in Fig. 2, inspection result data 202 contains the name of an inspected program, the name of a hash algorithm used for calculating a hash value of the program, and the calculated hash value. Inspection result data 202 also contains a list of the name of functions contained in the program and a list of information on resources accessed when the program is executed, which are obtained as a result of an analysis of the program using security evaluation list 201. The hash value contained in inspection result data 202 is used for verifying that the program has not been changed or falsified after inspection by program inspection device 20a.

[0025]

Fig. 3 is a block diagram illustrating a hardware configuration of mobile phone 50. CPU 501 executes a variety of programs stored in ROM 502 and nonvolatile memory 507, and thereby controls components of mobile phone 50. ROM 502 stores programs for controlling mobile phone 50. RAM 503 is used as a work area of CPU 501. Wireless communication unit 504, under the control of CPU 501, controls wireless communication with a base station (not shown) of mobile packet communication network 40. Operation input unit 505 consists of a plurality of keys, and outputs an operation signal to CPU 501 in response to an operation of the keys. Liquid crystal display unit 506 consists of a liquid crystal display panel and a driving circuit for controlling a display of the liquid crystal display panel.

[0026]

Nonvolatile memory 507 stores software such as an operating system and a WWW (World Wide Web) browser for mobile phone 50. Nonvolatile memory 507 also stores programs downloaded from content server 10a and stores inspection result data 202 thereof. Nonvolatile memory further stores security management table 507a.

[0027]

Security management table 507a, as shown in Fig. 4, registers, among functions contained in programs for mobile phone 50, the names of functions permitted to be used when a program received via a network is executed, and the names of functions not permitted to be used when a program received via a network is executed. Security management table 507a also registers, among resources accessible by mobile phone 50, information on resources permitted to be accessed when a program received via a network is executed, and information on resources not permitted to be accessed when a program received via a network is executed. As to a function and a resource which require asking a user whether to execute a program, a term "user confirmation" is registered in the item "permission" column of security management table 507a.

[0028]

Nonvolatile memory 507 stores a plurality of security management tables 507a for each security level available in mobile phone 50 such as security management table 507a for "Level 1" or security management table 507a for "Level 2". In mobile phone 50, when it is determined

5

whether to execute a program received via a network, security management table 507a corresponding to a security level presently set in mobile phone 50 is used among the plurality of security management tables 507a.    The security level is set by a user of mobile phone 50.

[0029]

Functions registered in security management table 507a and information on whether to permit uses of the functions may be changed by a user of mobile phone 50.    This is the same for resources registered in security management table 507a and information on whether to permit access of the resources.

[0030]

Operations of the first embodiment will now be described below.

Fig. 5 is a sequence chart illustrating operations of each component forming communication system 1, which are performed until a program and corresponding inspection result data 202 are downloaded to mobile phone 50.    As shown in Fig. 5, a program for mobile phone 50 written by content provider 10 is sent along with an inspection request from content server 10a to program inspection device 20a (Step S101).

[0031]

Program inspection device 20a, upon receipt of the program and the inspection request, analyzes the received program (Step S102).    Program inspection device 20a extracts from the program functions listed in security evaluation list 201, and identifies resources which are accessed if the program is executed, and which are listed in security evaluation list 201.    Program inspection device 20a also calculates a hash value of the program using a hash algorithm.    Program inspection device 20a then generates inspection result data 202 containing the names of the extracted functions, the information on the identified resources, the calculated hash value, the name of the algorithm used, and the file name of the program (Step S103).

[0032]

Subsequently, program inspection device 20a attaches an electronic signature to the generated inspection result data 202 (Step S104).    This electronic signature is used for verifying in mobile phone 50 that the program has not been changed or falsified.    After that, program inspection device 20a returns inspection result data 202 with the electronic signature to content server 10a (Step S105).    Content server 10a, upon receipt of inspection result data 202, stores inspection result data 202 with the inspected program in a memory (Step S106), and renders the program and inspection result data 202 downloadable by mobile phone 50.

[0033]

In mobile phone 50, a security level is set (Step S107).    In the setting of a security level, a screen shown in Fig. 6 is displayed on liquid crystal display unit 506, and a user can select a security level of mobile phone 50 from "Level 0 (Nothing)" to "Level 5" using operation input unit 505.    The security level set by the user is stored in nonvolatile memory 507.

[0034]

If mobile phone 50 downloads a program from content server 10a, a WWW browser is launched in mobile phone 50 (Step S108), and packet communications are started between mobile phone 50 and content server 10a.    When the user selects a program to be downloaded using operation input unit 505, a signal requesting download of the program is sent from mobile phone 50

to content server 10a (Step S109).   Content server 10a reads the requested program and inspection result data 202 of the program from memory, and sends them to mobile phone 50 (Steps S110 and S111) .   Mobile phone 50, upon receipt of the program and inspection result data 202, stores them in nonvolatile memory 507 (Step S112).

[0035]

Fig. 7 is a flowchart illustrating operations of determining whether to execute a program received via a network, and which are carried out in mobile phone 50.   The operations are carried out by CPU 501 if the execution of a program received via a network is instructed in mobile phone 50.   As shown in Fig. 7, CPU 501 reads from nonvolatile memory 207 inspection result data 202 of a program the execution of which has been instructed (Step S201).

[0036]

CPU 501 verifies an electronic signature of inspection result data 202 (Step S202), and thereby confirms that inspection result data 202 has been generated by inspection institution 20, and that inspection result data 202 is an authentic inspection result data which has not been falsified.   If, as a result of the verification of the electronic signature, it is found that inspection result data 202 is not authentic (Step S203: NO), CPU 501 cancels the execution of the program (Step S210), and causes liquid crystal display unit 506 to display a message stating that the execution of the program has been cancelled because falsification has been found in inspection result data 202.

[0037]

On the other hand, if inspection result data is verified to be authentic (Step S203: YES), CPU 501 calculates a hash value of the program using a hash algorithm described in inspection result data 202.   CPU 501 compares the calculated hash value and a hash value described in inspection result data 202 (Step S204).   As a result of the comparison, if the hash values do not match (Step S205: NO), CPU 501 cancels the execution of the program (Step S210), and causes liquid crystal display unit 506 to display a message stating that execution of the program has been cancelled because falsification has been found in the program.

[0038]

On the other hand, if the hash values match (Step S205: YES), CPU 501 identifies a value of a security level currently set in mobile phone 50, and reads from nonvolatile memory 507 security management table 507a corresponding to the identified value of the security level (Step S206).   CPU 501 compares the read security management table 507a and inspection result data 202 read in Step S201 (Step S207), and thereby determines whether to execute the program (Step S208).

[0039]

To explain the operations in Steps S207 and S208 specifically, CPU 501, for each function described in inspection result data 202, namely for each function extracted from the program to be executed, determines whether the function is a function permitted to be used in security management table 507a or a function prohibited from being used.   Similarly, CPU 501, for each resource described in inspection result data 202, determines whether the resource is a resource permitted to be accessed in security management table 507a or a resource prohibited from being used.

[0040]

7

As a result, if any function that are not permitted to be used is contained in inspection result data 202, or if any resource not permitted to be accessed is contained in inspection result data 202, CPU 501 determines that the program violates the security policy (security management table 507a) set by a user, and does not permit the execution of the program (Step S208: NO). Consequently, CPU 501 cancels the execution of the program (Step S210), and causes liquid crystal display unit 506 to display a message as shown in Fig. 8.

[0041]

For example, assuming that inspection result data 202 is as shown in Fig. 2 and security management table 507a is as shown in Fig. 4, since inspection result data 202 contains a function "Function 1 ()" which is not permitted to be used according to security management table 507a, and a resource "Local/UserData/AddressBook" which is not permitted to be accessed according to security management table 507a, a program corresponding to inspection result data 202 is not permitted to be executed in mobile phone 50.

[0042]

On the other hand, if all of the functions described in inspection result data 202 are functions that are permitted to be used according to security management table 507a, and all resources described in inspection result data 202 are resources permitted to be accessed according to security management table 507a, CPU 501 determines that the program meets the security policy set by the user, and permits the execution of the program (Step S208: YES).   Consequently, CPU 501 reads the program permitted to be executed from nonvolatile memory 507, launches the program (Step S209), and proceeds with operations in accordance with the program.

[0043]

If inspection result data 202 contains a resource requiring a user confirmation as a resource "http://www.xxx.co.jp" in security management table 507a of Fig. 4, CPU 501 generates a message asking a user whether to execute a program, causes liquid crystal display unit 506 to display it, and determines the execution of the program in accordance with an instruction from operation input unit 505.

[0044]

As stated above, in the present embodiment, program inspection device 20a pre-inspects the content of a program provided to mobile phone 50 via a network, and generates inspection result data 202 containing functions contained in the program and information on resources accessed when the program is executed.   Mobile phone 50 compares inspection result data 202 and security management table 507a registering information on whether a function may be used for each function and information on whether a resource may be accessed for each resource, and thereby determines whether to execute the program received via the network.   Accordingly, mobile phone 50, without analyzing the received program, only by comparing inspection result data 202 and security management table 507a, can determine whether the program meets the security policy (security management table 507a) set in mobile phone 50.   Consequently, the determination process can be completed in mobile phone 50 by using a simple method and within a short time.

[0045]

Security management table 507a for determining whether to execute a received program can be changed easily by changing a security level.   Accordingly, even if a program violates a

security policy and thereby is determined not permitted to be executed, if a user determines that the program is valid, the program can be executed in mobile phone by temporarily lowering the security level.    As stated above, in the present embodiment, flexible setting of a security level of mobile phone 50 relative to a received program can be carried out in accordance with a user's wishes.

[0046]

[B. Second Embodiment]

Below, the second embodiment of the present invention will be described.

In the present embodiment, elements common to the first embodiment are denoted by like symbols, and descriptions common to the first embodiment will be omitted.

[0047]

Fig. 9 is a block diagram illustrating a hardware configuration of relay device 60 relaying packet communications between content server 10a and mobile phone 50.    Relay device 60 may be provided on either of Internet 30 or mobile packet communication network 40.    In Fig. 9, communication interface 604, under the control of CPU 601, controls packet communication with content server 10a or mobile phone 50.    Operation input unit 605 has a mouse and a keyboard, and outputs an operation signal to CPU 601 in accordance with operations carried out via the mouse and the keyboard.    Display unit 606 is a LCD or CRT display.

[0048]

HD (Hard Disk) 607 stores security management table 507a explained in the first embodiment.    Relay device 60 of the present embodiment, using security management table 507a, determines whether to relay a program sent from content server 10a to mobile phone 50.    Relay device 60 receives, along with the program, inspection result data 202 of the program and destination information indicating the destination of the program from content server 10a. Inspection result data 202 is generated by program inspection device 20a explained in the first embodiment.    The address information is a communication address assigned to mobile phone 50 such as an IP address.

[0049]

In the present embodiment, a security level in relay device 60 is set by a carrier of mobile packet communication network or an administrator of relay device 60.    HD 607 stores different security management tables 507a for each security level as described in the first embodiment, and in accordance with the security level set in relay device 60, security management table 507a for determining whether to relay a program is determined.

[0050]

Fig. 10 is a flowchart illustrating operations performed for determining whether to relay a program which are carried out in relay device 60.    The operations are performed by CPU 601 if relay device 60 receives a program and inspection result data 202 thereof transmitted from content server 10a to mobile phone 50.    As shown in Fig. 10, CPU 601 verifies an electronic signature of inspection result data 202 (Step S301).    If upon verification of the electronic signature, it is confirmed that inspection result data 202 is not authentic (Step S302: NO), CPU 601 cancels transfer of the program to mobile phone 50 (Step S309), and sends to mobile phone 50 a message stating that the download of the program has been cancelled because falsification has been found in inspection result data 202.

[0051]

On the other hand, if inspection result data is verified to be authentic (Step S302: YES), CPU 601 calculates a hash value of the program using a hash algorithm described in inspection result data 202, and compares the calculated hash value and a hash value described in inspection result data 202 (Step S303).    If as a result of the comparison, it is determined that the hash values do not match (Step S304: NO), CPU 601 cancels transfer of the program to mobile phone 50 (Step S309), and sends to mobile phone 50 a message stating that download of the program has been cancelled because falsification has been found in the program.

[0052]

On the other hand, if the hash values match (Step S304: YES), CPU 601 identifies a value of a security level set in relay device 60 at the time, and reads from HD 607 security management table 507a corresponding to the identified value of the security (Step S305).    CPU 601 compares the read security management table 507a and the received inspection result data 202 (Step S306), and thereby determines whether to relay the program to mobile phone 50 (Step S307).

[0053]

To explain the operations in Steps S306 and S307 specifically, CPU 601, for each function described in inspection result data 202, namely for each function extracted from the received program, determines whether the function is a function permitted to be used or a function prohibited from being used, according to security management table 507a.    Similarly, CPU 601, for each resource described in inspection result data 202, determines whether the resource is a resource permitted to be accessed or a resource prohibited from being used, according to security management table 507a.

[0054]

As a result, if any functions that are not permitted to be used exist  in inspection result data 202, or if any resources that are not permitted to be accessed exist in inspection result data 202, CPU 601 determines that the program violates the security policy (security management table 507a) set by, for example a carrier of mobile packet communication network 40, and does not permit relay of the program to mobile phone 50 (Step S307: NO).    Consequently, CPU 601 cancels the transfer of the program (Step S309), and sends to mobile phone 50 a message stating that the download of the program has been cancelled.

[0055]

On the other hand, if all functions described in inspection result data 202 are functions permitted to be used according to security management table 507a, and all resources described in inspection result data 202 are resources permitted to be accessed according to security management table 507a, CPU 601 determines that the received program meets the security policy set by the carrier of mobile packet communication network 40, and permits the relay of the program to mobile phone 50 (Step S307: YES).    Consequently, CPU 601 transfers the program to mobile phone 50 designated by the address information (Step S308).

[0056]

As stated above, in the present embodiment, program inspection device 20a pre-inspects the content of a program provided to mobile phone 50 via a network, and generates inspection result data 202 containing functions contained in the program and information on resources accessed

when the program is executed.    Relay device 60 compares inspection result data 202 and security management table 507a registering information for each function on whether that function may be used and information on each resource on whether that resource may be accessed; and thereby determines whether to relay the program to mobile phone 50.    Accordingly, relay device 60, without analyzing the program to be relayed, only by comparing inspection result data 202 and security management table 507a, can determine whether the program meets the security policy (security management table 507a) set in relay device 60.    Consequently, the determination process can be completed in relay device 60 by using a simple method and within a short time, thereby avoiding any delay in communications.    Also, since transfer of a program violating a security policy is cancelled, provision of such a program to mobile phone 50 is prevented.

[0057]

Functions registered in security management table 507a and information on which functions may be used can be changed by a carrier of mobile packet communication network 40 or by an administrator of relay device 60.    This is the same for resources registered in security management table 507a and information on which resources may be accessed.

[0058]

[C. Modifications]

(1)    In the first embodiment, inspection result data 202 is sent to mobile phone 50 along with a program.    However, as shown in Fig. 11, there may be provided inspection result registering server 70 for registering inspection result data 202 of each program inspected in inspection institution 20. In this case, mobile phone 50, after downloading a program from content server 10b, obtains inspection result data 202 of the program from inspection result registering server 70.    This is the same as in the second embodiment, namely, inspection result registering server 70 registers inspection result data 202 of each program, and relay device 60, if receiving a program to be transferred to mobile phone 50 from content server 10b, obtains inspection result data 202 of the program from inspection result registering server 70.    Inspection result registering server 70 may be provided either on mobile packet communication network 40 or in inspection institution 20.

[0059]

(2)    In the first embodiment, when a determination in Step S208 of Fig. 7 is negative, operations may be changed as shown in Fig. 12.

Namely, CPU 501, if a determination in Step S208 of Fig. 7 is negative, causes liquid crystal display unit 506 to display, as shown in Fig. 13, a message that a program to be executed violates a security policy, and a message confirming whether the program should be executed with available functions limited (Step S401).    Responsive to these messages, a user instructs mobile phone 50 using operation input unit 505 to execute the program with available functions limited or to cancel execution of the program.    The messages may be outputted as voice messages from mobile phone 50.

[0060]

CPU 501, if canceling execution of the program is instructed via operation input unit 505 (Step S402: NO), cancels execution of the program (Step S403).    On the other hand, if execution of the program is instructed via operation input unit 505 (Step S402: YES), CPU 501 reads the program from nonvolatile memory 507 and launches it (Step S404).    After that, CPU 501

11

determines whether the running program has been terminated (Step S405), and until termination of the running program, limits functions available in the program in accordance with security management table 507a (Step S406).    Security management table 507a for limiting available functions corresponds to a security level set in mobile phone 50 at that time.

[0061]

To explain the operations in Step S406 specifically, if CPU 501 identifies a function such as a function call and a system call when sequentially interpreting and running the program, CPU 501 determines whether the function is a function permitted to be used or a function prohibited from being used, according to security management table 507a.    If the function is a function permitted to be used, CPU 501 permits the use of the function and continues the running of the program.    On the other hand, if the function is a function not permitted to be used, CPU 501 does not permit the use of the function and suspends the running of the program.

[0062]

Also, CPU 501 monitors an access request to a resource occurring when sequentially interpreting and running the program, and determines whether the resource for the access request is a resource permitted to be accessed or a resource prohibited from being accessed, according to security management table 507a.    If the resource is a resource permitted to be accessed, CPU 501 permits an access to the resource and continues the running of the program.    On the other hand, if the resource is a resource not permitted to be accessed, CPU 501 does not permit an access to the resource and suspends the running of the program.

[0063]

According to the configuration stated above, mobile phone 50 can execute even a program violating a security policy by limiting available functions of the program.

[0064]

(3)    Security management table 507a may register only functions permitted to be used and those not permitted to be used; while security management table 507a may register only information on resources permitted to be accessed and those not permitted to be accessed.    Further, security management table 507a may register only functions permitted to be used or only functions not permitted to be used; while security management table 507a may register only resources permitted to be accessed or only resources not permitted to be accessed.

[0065]

(4)    In the second embodiment, HD 607 of relay device 60 may register for each mobile phone 50 a security level set by a user of mobile phone 50.    In this case, relay device 60 may identify a security level of mobile phone 50 to which a program is to be transferred, and determine whether to relay the program using security management table 507a corresponding to the security level.

[0066]

(5)    In the first embodiment, nonvolatile memory 507 of mobile phone 50 may store a security management table for a program to which inspection result data 202 has not been attached.    Also, nonvolatile memory 507, if there are a plurality of inspection institutions similar to inspection institution 20, may store a security management table for a program to which inspection result data generated in an inspection institution other than inspection institution 20 has been attached.    This is the as same in the second embodiment; namely, HD 607 may store a security management table

for a program to which inspection result data 202 has not been attached, or a security management table for a program to which inspection result data generated in an inspection institution other than inspection institution 20 has been attached.

[0067]

(6)      In the first embodiment, inspection result data 202 may further contain provider identification information for identifying a provider of a program such as the name of a content provider or a URL of a program sending source; and nonvolatile memory 507 of mobile phone 50 may store different security management tables 507a for each provider identification information. In this case, mobile phone 50 may determine whether to execute a received program using security management table 507a corresponding to a provider identification information contained in received inspection result data 202.   This is the same in the second embodiment, namely, inspection result data 202 may further contain a provider identification information, HD 607 of relay device 60 may store different security management tables 507a for each provider identification information; and relay device 60 may determine whether to relay a received program using security management table 507a corresponding to a provider identification information contained in received inspection result data 202.

[0068]

(7)      In the first embodiment, mobile phone 50, on completion of downloading a program, may determine whether the program meets a security policy (security management table 507a) by comparing inspection result data 202 of the program and security management table 507a, and cause liquid crystal display unit 506 to display the determination result.   The determination result may be outputted as voice messages from mobile phone 50.   Also, mobile phone 50, when instructed by a user using operation input unit 505 to check the safety of a received program, may determine whether the program meets a security policy by comparing inspection result data 202 of the program and security management table 507a, and output the determination result.

[0069]

In the cases stated above where a determination is made not as to whether program should be executed but as to whether the program meets a security policy, and the determination result is reported to a user, the user, on the basis of the reported determination result, deletes (uninstalls) the program from nonvolatile memory 507 or avoids execution of the program, which consequently maintains the security of mobile phone 50.   In this case, if the program violates the security policy, the names of functions not permitted to be used and information on resources not permitted to be accessed, which are contained in the program, may be reported to the user along with the determination result.   Alternatively, if the program violates the security policy, mobile phone 50 may cause liquid crystal display unit 506 to display a message confirming whether to delete the program, and if instructed by use of operation input unit 505 to delete the program, will uninstall the program from nonvolatile memory 507.

[0070]

In the second embodiment, relay device 60, when transferring a program to mobile phone 50, may determine whether the program meets a security policy (security management table 507a) by comparing inspection result data 202 of the program and security management table 507a, and send the determination data to mobile phone 50 along with the program.

[0071]

(8)    In the first embodiment, mobile phone 50, before downloading a program from content server 10a, may download only inspection result data 202 of the program from content server 10a. In this case, mobile phone 50 compares received inspection result data 202 and security management table 507a, and thereby determines whether the program to be downloaded meets a security policy (security management table 507a).    As a result of the determination, if the program meets the security policy, mobile phone 50 downloads the program from content server 10a.    On the other hand, if the program violates the security policy, mobile phone 50 cancels download of the program.    According to this configuration, if a program to be downloaded violates a security policy, downloading the program is prevented, and consequently unnecessary packet communications can be avoided.

[0072]

(9)    In the first and second embodiment, a program may be distributed to mobile phone 50 instead of being downloaded.    A receiving device according to the present invention may be applied to a wireless terminal communicating via a public wireless LAN or a personal computer communicating via the Internet.    A relay device according to the present invention may be applied to a gateway server, a proxy server, or a switching center or a base station provided on mobile packet communication network 40.    A program for causing a computer such as mobile phone 50 or relay device 60 to execute processes according to the present invention may be installed in a computer via a network, or may be stored in a variety of computer-readable storage media for distribution.

[Brief Description of the Drawings]

[0073]

Fig. 1 is a block diagram illustrating a configuration of a communication system according to the first embodiment.

Fig. 2 is a diagram illustrating a data structure of inspection result data 202 according to the first embodiment.

Fig. 3 is a block diagram illustrating a hardware configuration of mobile phone 50 according to the first embodiment.

Fig. 4 is a diagram illustrating a data structure of security management table 507a according to the first embodiment.

Fig. 5 is a sequence chart illustrating operations of each component forming communication system 1 according to the first embodiment, which are performed until a program and inspection result data 202 thereof are downloaded to mobile phone 50.

Fig. 6 is a diagram illustrating a screen displayed on a mobile phone 50 when a security level is set according to the first embodiment.

Fig. 7 is a flowchart illustrating operations for determining whether to execute a program received via a network, which operations are carried out in mobile phone 50 according to the first embodiment.

Fig. 8 is a diagram illustrating a screen displayed on mobile phone 50 when execution of a program is not permitted according to the first embodiment.

Fig. 9 is a block diagram illustrating a hardware configuration of relay device 60 according

to the second embodiment.

　　Fig. 10 is a flowchart illustrating operations of determining whether to execute a program received via a network, which operations are carried out in relay device 60 according to the second embodiment.

　　Fig. 11 is a block diagram illustrating a configuration of communication system 2 according to the modification (1).

　　Fig. 12 is a flowchart illustrating operations carried out in mobile phone according to the modification (2).

　　Fig. 13 is a diagram illustrating a screen displayed on mobile phone 50 according to the modification (2).

[Concise Description of Symbols]

　　[0074]

　　1, 2 --- Communication System, 10 --- Content Provider, 10a, 10b --- Content Server, 20 --- Inspection Institution, 20a --- Program Inspection Device, 30 --- Internet, 40 --- Mobile Packet Communication Network, 50 --- Mobile Phone, 60 --- Relay Device, 70 --- Inspection Result Registering Server, 201 --- Security Evaluation List, 202 --- Inspection Result Data, 501 --- CPU, 502 --- ROM, 503 --- RAM, 504 --- Wireless Communication Unit, 505 --- Operation Input Unit, 506 --- Liquid Crystal Display Unit, 507 --- Nonvolatile Memory, 507a --- Security Management Table, 601 --- CPU, 602 --- ROM, 603 --- RAM, 604 --- Communication Interface, 605 --- Operation Input Unit, 606 --- Display Unit, 607 --- HD.

*FIG. 1*

1 : COMMUNICATION SYSTEM

MOBILE PACKET COMMUNICATION NETWORK

40

50

20 INSPECTION INSTITUTION

PROGRAM INSPECTION DEVICE 20a

SECURITY EVALUATION LIST 201

INTERNET

30

10 CONTENT PROVIDER

CONTENT SERVER

PROGRAM 10a

+

INSPECTION RESULT DATA 202

*FIG. 2*
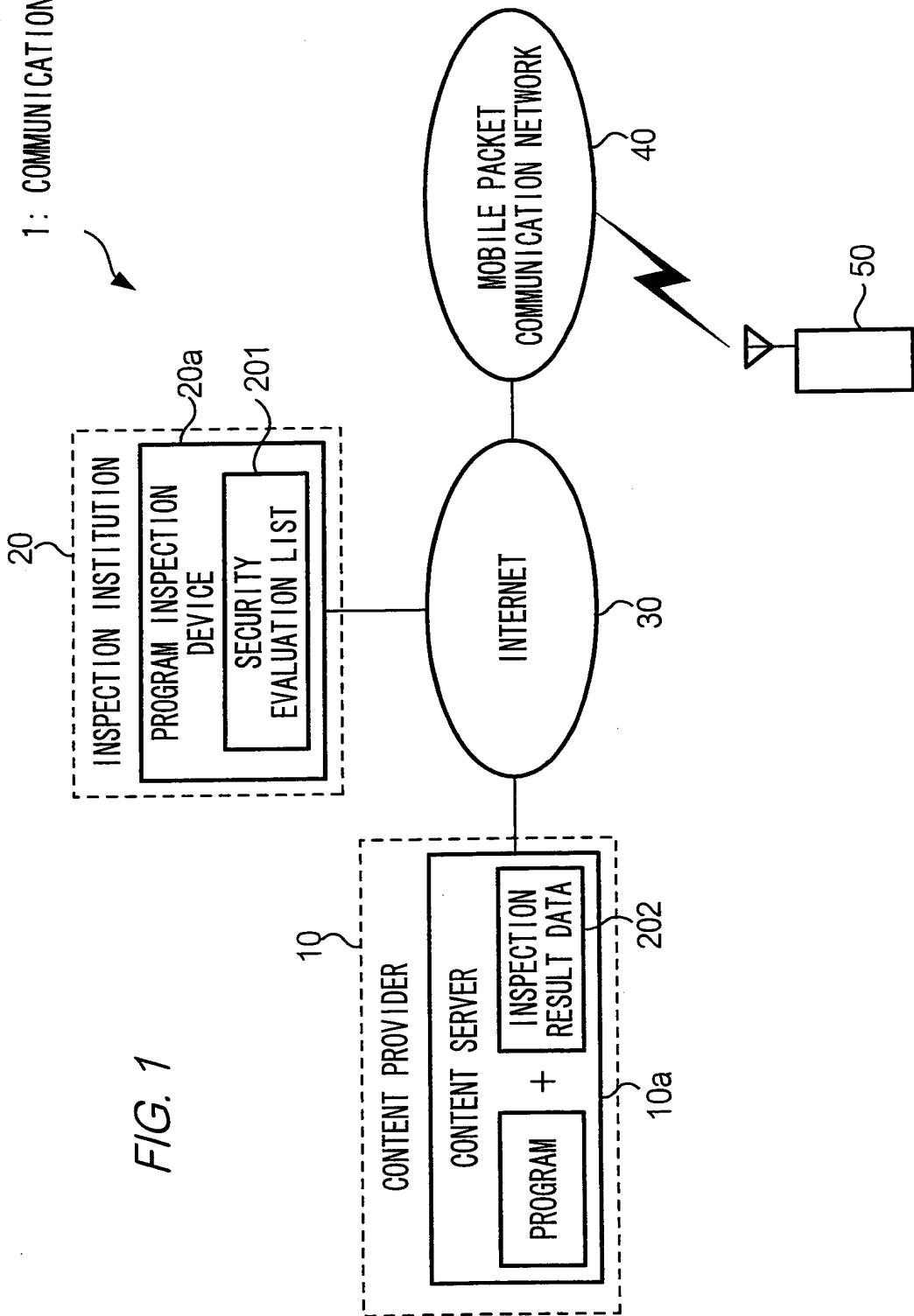
202: INSPECTION RESULT DATA

| PROGRAM | Sample.APP | | |
|---|---|---|---|
| HASH ALGORITHM | MD5 | | |
| HASH ALGORITHM | 0D247FCB001A2BC5FED0000009355FF23 | | |
| FUNCTION | FUNCTION NAME | | |
| | Function 1 ( ) | | |
| | Function 2 ( ) | | |
| | Function 5 ( ) | | |
| | ...... | | |
| ACCESSED RESOURCE | TYPE | | RESOURCE |
| | Network | | http://www.xxx.co.jp |
| | File | | Local/UserData/AddressBook |
| | ...... | | ...... |

50: MOBILE PHONE  *FIG. 3*

| 501 | 502 | 503 | 504 |
|---|---|---|---|
| CPU | ROM | RAM | WIRELESS COMMUNICATION UNIT |

| OPERATION INPUT UNIT | LIQUID CRYSTAL DISPLAY UNIT | NONVOLATILE MEMORY |
|---|---|---|
| | | SECURITY MANAGEMENT TABLE |

505   506   507   507a

60: RELAY DEVICE  *FIG. 9*

| 601 | 602 | 603 | 604 |
|---|---|---|---|
| CPU | ROM | RAM | COMMUNICATION INTERFACE |

| OPERATION INPUT UNIT | DISPLAY UNIT | HD |
|---|---|---|
| | | SECURITY MANAGEMENT TABLE |

605   606   607   507a
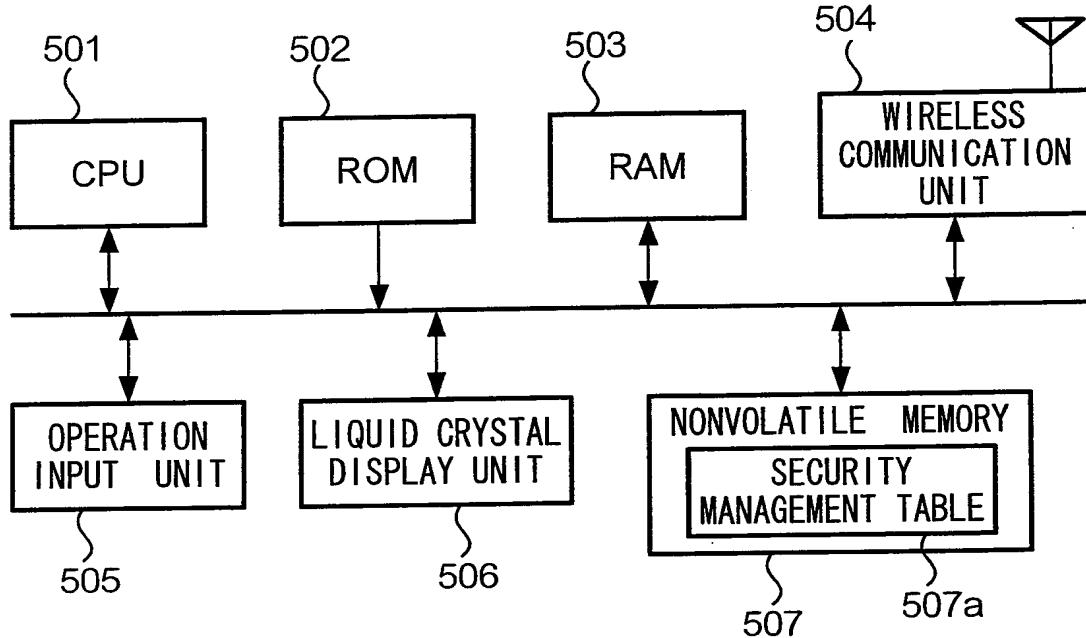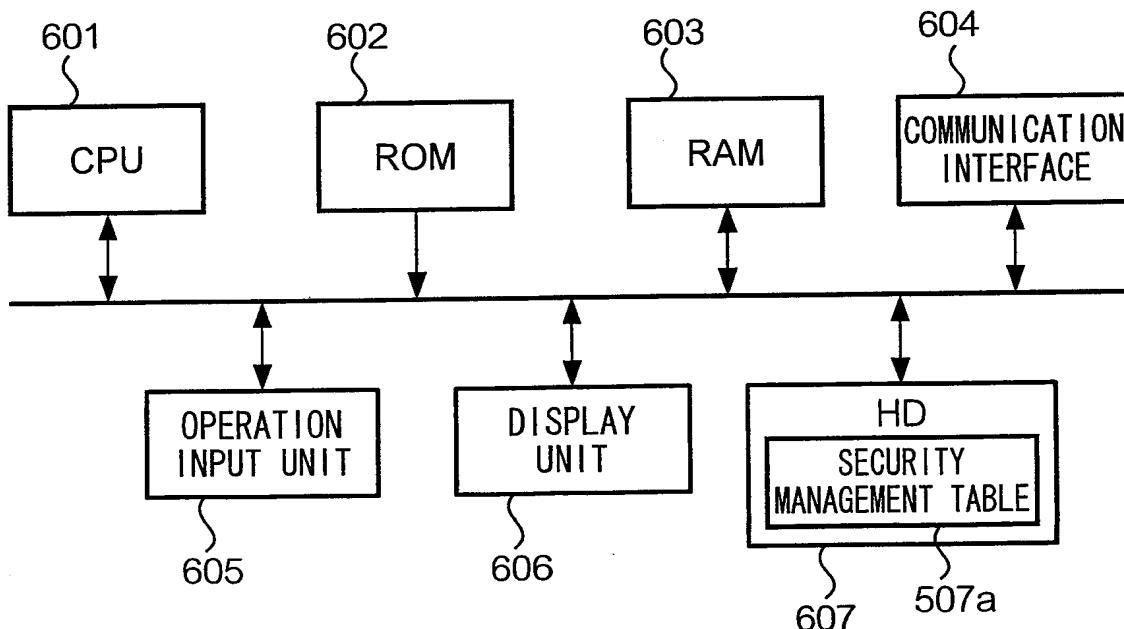
## FIG. 4

507a: SECURITY MANAGEMENT TABLE

| SECURITY LEVEL | LEVEL1 | | |
|---|---|---|---|
| FUNCTION | CATEGORY | FUNCTION NAME | PERMISSION |
| | FILE ACCESS | Function 1 ( ) | PROHIBITED |
| | | Function 2 ( ) | PERMITTED |
| | NETWORK ACCESS | ALL FUNCTIONS | PROHIBITED |
| | ...... | ...... | ...... |
| ACCESSED RESOURCE | TYPE | RESOURCE | PERMISSION |
| | Network | http://www.xxx.co.jp | USER CONFIRMATION |
| | Data File | ALL DATA FILES | PROHIBITED |
| | File | Local/UserData/AddressBook | PROHIBITED |
| | ...... | ...... | ...... |

*FIG. 5*

*FIG. 6*

HIGH        LEVEL 5

            LEVEL 4

            LEVEL 3

SECURITY
            LEVEL 2

            LEVEL 1

LOW         LEVEL 0
            (NOTHING)

SET SECURITY LEVEL

【REGISTER】

*FIG. 8*

WARNING

EXECUTION OF THIS PROGRAM IS
CANCELLED BECAUSE IT VIOLATES
SECURITY POLICY SET BY YOU.

【RETURN】

【CHECK SECURITY POLICY】

*FIG. 7*

```
                    ┌─────────────┐
                    │    START    │
                    └─────────────┘
                           │
                           ▼
S201        ┌──────────────────────────────┐
            │   OBTAIN INSPECTION          │
            │   RESULT DATA 202            │
            └──────────────────────────────┘
                           │
                           ▼
S202        ┌──────────────────────────────┐
            │   VERIFY ELECTRONIC          │
            │   SIGNATURE                  │
            └──────────────────────────────┘
                           │
                           ▼
S203        ╱──────────────────────╲      NO
            ╲      VERIFIED?        ╱ ─────────────┐
             ╲────────────────────╱               │
                      │ YES                        │
                      ▼                            │
S204        ┌──────────────────────────────┐       │
            │   COMPARE HASH VALUES        │       │
            └──────────────────────────────┘       │
                      │                            │
                      ▼                            │
S205        ╱──────────────────────╲      NO        │
            ╲       MATCH?         ╱ ─────────────┐ │
             ╲────────────────────╱             │ │
                      │ YES                      │ │
                      ▼                          │ │
S206        ┌──────────────────────────────┐     │ │
            │   IDENTIFY SECURITY          │     │ │
            │   MANAGEMENT TABLE 507a      │     │ │
            └──────────────────────────────┘     │ │
                      │                          │ │
                      ▼                          │ │
S207        ┌──────────────────────────────┐     │ │
            │  COMPARE WITH INSPECTION     │     │ │
            │  RESULT DATA 202             │     │ │
            └──────────────────────────────┘     │ │
                      │                          │ │
                      ▼                          │ │
S208        ╱──────────────────────╲    NO        │ │
            ╲     EXECUTION        ╱ ───────────┐ │ │
            ╱     PERMITTED?       ╲           │ │ │
             ╲────────────────────╱            │ │ │
                      │ YES                     │ │ │
                      ▼              S210        ▼ ▼ ▼
S209        ┌────────────────┐   ┌──────────────────┐
            │ EXECUTE PROGRAM│   │ CANCEL EXECUTION │
            └────────────────┘   └──────────────────┘
                      │                   │
                      ▼◄──────────────────┘
                ┌─────────────┐
                │     END     │
                └─────────────┘
```

*FIG. 10*

```
        ┌─────────────┐
        │    START    │
        └─────────────┘
               │
               ▼
S301  ┌─────────────────────┐
      │  VERIFY ELECTRONIC  │
      │     SIGNATURE       │
      └─────────────────────┘
               │
               ▼
S302    ╱───────────────╲       NO
       ⟨    VERIFIED?    ⟩──────────┐
        ╲───────────────╱          │
               │ YES               │
               ▼                   │
S303  ┌─────────────────────┐      │
      │ COMPARE HASH VALUES │      │
      └─────────────────────┘      │
               │                   │
               ▼                   │
S304    ╱───────────────╲    NO    │
       ⟨     MATCH?      ⟩─────────►│
        ╲───────────────╱          │
               │ YES               │
               ▼                   │
S305  ┌─────────────────────┐      │
      │ IDENTIFY SECURITY   │      │
      │ MANAGEMENT TABLE 507a│     │
      └─────────────────────┘      │
               │                   │
               ▼                   │
S306  ┌─────────────────────┐      │
      │COMPARE WITH INSPECTION│    │
      │  RESULT DATA 202     │      │
      └─────────────────────┘      │
               │                   │
               ▼                   │
S307    ╱───────────────╲    NO    │
       ⟨ RELAY PERMITTED?⟩─────────►│
        ╲───────────────╱          │
               │ YES          S309 ▼
               ▼            ┌─────────────────┐
S308  ┌─────────────────┐  │ CANCEL TRANSFER │
      │ TRANSFER PROGRAM│  └─────────────────┘
      └─────────────────┘           │
               │                    │
               ▼◄───────────────────┘
        ┌─────────────┐
        │     END     │
        └─────────────┘
```

*FIG. 11*

2: COMMUNICATION SYSTEM

MOBILE PACKET COMMUNICATION NETWORK 40

MOBILE PHONE 50

INSPECTION INSTITUTION 20

PROGRAM INSPECTION DEVICE 20a

SECURITY EVALUATION LIST 201

INTERNET 30

INSPECTION RESULT REGISTERING SERVER 70

INSPECTION RESULT DATA 202

CONTENT PROVIDER 10

CONTENT SERVER

PROGRAM 10b

*FIG. 12*

STEP S208 : NO

S401 — DISPLAY MESSAGE

S402 — LIMIT FUNCTIONS —— NO

YES

S404 — LAUNCH PROGRAM

S403 — CANCEL EXECUTION

S405 — TERMINATED? —— YES

NO

S406 — LIMIT AVAILABLE FUNCTIONS IN ACCORDANCE WITH SECURITY MANAGEMENT TABLE 507a

END

*FIG. 13*

THIS PROGRAM VIOLATES SECURITY POLICY.
LIMIT AVAILABLE FUNCTIONS AND EXECUTE PROGRAM?

【EXECUTION】        【CANCEL】

[Document Name] Abstract

[Abstract]

[Problem] To determine, in a receiving device or a relay device, using a simple method and within a short time, whether a program provided via a network is a program causing security concerns.

[Solution] Program inspection device 20a pre-inspects the content of a program provided to mobile phone 50 via a network, and generates inspection result data 202 containing functions contained in the program and information on resources accessed when the program is executed.   Mobile phone 50 has security management table 507a registering information for each function on whether the function may be used and information on whether a resource may be accessed for each resource. Mobile phone 50 compares inspection result data 202 of a program received via a network and security management table 507a, and thereby confirms whether the program causes security concerns when it is executed.

[Selected View] Fig. 1